Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 06 February 2004

Current Nationwide Threat Level is

ELEVATED

SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here

www.whitehouse.gov/homeland

Daily Overview

- The Washington Post reports Congress is expanding its focus on the growing business of online fraud with the introduction of new legislation that would mandate stiffer sentences for anyone who commits a crime using a Website registered under a false name. (See item 4)
- Reuters reports a panel of international experts has said there is a "high probability" of more cases of bovine spongiform encephaopathy in U.S. cattle. (See item 15)
- US−CERT has released "Technical Cyber Security Alert TA04−036A: HTTP Parsing Vulnerabilities in Check Point Firewall−1." (See item 23)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base

Service Industries: Banking and Finance; Transportation; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information and Telecommunications; Internet Alert Dashboard

Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *February 05, KOIN.com (OR)* — **Power goes off in Portland after explosion. Nine downtown buildings in Portland, OR, were in the dark Wednesday night so crews could inspect damage after an afternoon explosion. About 1:15 p.m., a transformer exploded under the sidewalk** outside the Smart Park garage at Southwest Second and Jefferson streets. **The underground blast rocked nearby buildings, including the Edith Green/Wendall Wyatt Federal Building,** blew a metal grate into the air, and knocked out a window. Portland General Electric cut the power at 7:08 p.m. to several buildings so crews could safely inspect

the underground switch that failed. The outage lasted less than an hour.
Source: http://www.koin.com/webnews/2004/20040205_explosion.shtml

2. *February 05, National Nuclear Security Administration* — **U.S. launches effort to detect terrorist shipments of nuclear and radioactive material. The U.S. and Lithuanian governments announced on Thursday, February 5, the two countries will work together in the war on terrorism by installing special equipment at the Vilnius Airport to detect hidden shipments of nuclear and other radioactive material.** This is part of a new effort to extend to international airports the National Nuclear Security Administration's (NNSA) successful "Megaports" program that installs sophisticated detection equipment at many of the world's ports. For the past two years, U.S. technical experts have worked with Lithuania, Vilnius Airport staff, and Lithuanian private industry to install radiation detection systems that will assist in detection, deterrence, and interdiction of illicitly− trafficked nuclear and other radioactive materials. **The specialized radiation−detection technology is part of the overall U.S. nuclear security program to guard against proliferation of weapons materials.**
Source: http://releases.usnewswire.com/GetRelease.asp?id=136−0205200 4

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *February 05, Government Computer News* — **Admiral says the future of the Navy lies in integration. Admiral Vern Clark, the chief of Naval Operations, foresees a Navy that needs fewer people to accomplish its mission as it relies more on speed and agility. It will achieve this goal, he says, by integrating more efficiently with the Army, Air Force and Marine Corps** and by taking advantage of their IT investments. Clark's vision of the Navy could include mergers with other services in operations such as intelligence, and it must include a faster, more collaborative acquisition process, he said. The Department of Defense is working to improve the speed at which military services acquire new technologies and weapons, he said. Clark said he is eager to receive suggestions from industry on how the military services can break down stovepipes and fight as one force.
Source: http://www.gcn.com/vol1_no1/daily−updates/24853−1.html

[Return to top]

Banking and Finance Sector

4. *February 04, Washington Post* — **Congress eyes Internet fraud crackdown. Congress is expanding its focus on the growing business of online fraud with the introduction of new legislation that would mandate stiffer sentences for anyone who commits a crime using a Website registered under a false name.** The "Fraudulent Online Identity Sanctions Act,"

sponsored by Reps. Lamar Smith and Howard Berman, would add as much as seven years to prison sentences handed out to anyone committing fraud through a Website registered under a false name or contact in formation. Smith and Berman drafted the bill after receiving complaints from the entertainment and software industries that much of their material is made available for free on Websites whose owners are impossible to track down because their domain name registrations often contain made−up names like "John Doe" and phone numbers like "123−4567." The information is stored in public "whois" databases that are run by registrars, the businesses that sell Internet addresses. **The proposal could run up against opposition from privacy advocates who say that information like home addresses and telephone numbers should not be made available if the registrant does not want it revealed.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A13538−2004Feb 4.html

[Return to top]

Transportation Sector

5. *February 05, Federal Computer Week* — **House bill stresses smart transport.** In a session today, February 5, the House Science Committee approved a transportation research bill that emphasizes development of intelligent transportation systems: the Surface Transportation Research and Development Act of 2004. **Intelligent transportation systems (ITS) in development by the Transportation Department include the 511 traveler information service, the Vehicle Infrastructure Integration program, a wireless enhanced 911 system and the integration of transportation systems into the issuance of the AMBER Alert program.** In December, the Federal Communications Commission moved forward in a decision to license the dedicated short range communications technology, which is used between vehicles and roadside devices, or vehicles in close range. One possible use of this technology is for the development of intelligent intersections, at which drivers could be warned of a potential crash as they approach an intersection. Transportation Department officials hope to make this technology available in 2005.
Source: http://www.fcw.com/fcw/articles/2004/0202/web−smart−02−04−04 .asp

6. *February 05, Federal Computer Week* — **U.S. Coast Guard faces communications hurdles.** Despite large advances in defense communications technologies during the past several years, the U.S. Coast Guard must still overcome large communications barriers with the Defense Department's services, said Vice Adm. Terry Cross, commander of the Coast Guard's Pacific Fleet. Speaking at the West 2004 conference, sponsored by AFCEA and the U.S. Naval Institute, Cross said the maritime communications technology afforded to the Coast Guard must advance at a pace comparable to its DOD counterparts. **Coast Guard officials also face the unique challenge of dealing with both the .gov space used by the Homeland Security Department and the .mil domain of DOD.** Cross said that on September 11, 2001, only the largest tactical units of the Coast Guard had access to the Secure Internet Protocol Routing Network, the secure DOD communications network. But a great deal of money spent over the last few years has brought the Coast Guard in closer alignment with DOD. "The real challenge is in [command, control, communications, computers, intelligence, surveillance and reconnaissance]." Cross said. "C4ISR must be jointly capable as the Coast Guard, Navy and Marine Corps train together."

Source: http://fcw.com/fcw/articles/2004/0202/web−coast−02−03−04.asp

7. *February 05, Associated Press* — **Amtrak adds wireless Internet at stations.** Amtrak will soon offer Internet access at some of its busiest stations, allowing passengers waiting for the train to check their e−mail or surf the Net. The railroad said Thursday, February 5, that it has signed an agreement to offer high−speed wireless Internet access, also known as WiFi, at six stations along the Northeast corridor. **The six stations are: Boston's Route 128 Station; Providence, R.I.; New York Penn Station; Philadelphia's 30th Street Station; Wilmington, Del.; and Baltimore's Penn Station. Amtrak spokesperson Marcie Golgoski says any passengers with a WiFi−enabled laptop or PDA will be able to access the system as soon as they walk into the station.** The new service will be available early this summer.
Source: http://cbsnewyork.com/topstories/topstoriesny_story_03616423 8.html

8. *February 05, Associated Press* — **Seattle airport security screening supervisor put on leave. An airport security screening supervisor has been placed on administrative leave pending an investigation into accusations that he took money from other workers seeking promotions.** Kevin Morris, an acting manager at Seattle−Tacoma International Airport (Sea−Tac), was placed on indefinite paid leave Wednesday at the direction of Transportation Security Administration (TSA) officials in Washington, DC, agency spokesperson Jennifer Marty said. The order overrode a decision by the agency's Sea−Tac director, Robert Blunk, to let Morris remain at work because Morris was not in a position to choose those who were promoted. **In a letter to TSA made public earlier this week, 206 of the agency's 1,100 workers at Sea−Tac wrote that other employees paid Morris $300 each to help them complete applications for promotions.**
Source: http://www.kgw.com/sharedcontent/APStories/stories/D80H8RCO0 .html

9. *February 05, National Journal's Technology Daily* — **Bush calls for increased budget for seaport security initiatives.** President Bush on Friday touted increased funding for seaport security initiatives in his fiscal 2005 budget proposal. Bush's budget request unveiled on Monday, February 2, includes $1.9 billion for the Homeland Security Department's port security efforts −− an increase of 13 percent compared to the fiscal 2004 level. **The president also highlighted the department's program to screen ship cargo before it leaves foreign ports. Under the president's plan, the Container Security Initiative would receive a boost of $25 million from the previous fiscal year.** For seaport security, the budget also includes: $102 million for the Coast Guard security efforts; $50 million for advanced screening devices and $20.6 million to bolster staffing and technology at the nation's operation center for seaport security. For details, also see: http://www.dhs.gov/dhspublic/display?content=3129
Source: http://www.govexec.com/dailyfed/0204/020504tdpm1.htm

10. *February 04, U.S. Coast Guard* — **Coast Guard receives majority of maritime security plans.** The U.S. Coast Guard has announced that 90 percent of vessels and port facilities turned in security plans as required by the Maritime Transportation Security Act. Penalties are being issued to those that have not submitted any of the information required. Though most have complied, the Coast Guard will be aggressively pursuing those who did not. “Security in America’s ports is a shared responsibility,” said Rear Adm. Larry Hereth, director of port security for the Coast Guard. **Designed to protect the nation’s ports and waterways from a terrorist attack, the act requires the development and implementation of security plans**

for vessels and facilities that have a higher risk of involvement in a transportation security incident. The act also mandates that all affected vessels and facilities be in compliance by July 1, and timely security plan submission is a key milestone in reaching that goal. **Under the act, large cargo and passenger vessels, port facilities, outer continental shelf facilities, and others in the maritime industry were required to submit a vulnerability assessment report and a security plan.**
Source: https://www.piersystem.com/external/index.cfm?cid=651&fuseaction=EXTERNAL.docview&pressid=29036

[Return to top]

Postal and Shipping Sector

11. *February 05, Washington Post* — **Mail search yields no direct ricin links. Investigators have finished examining letters and envelopes from the office of Senate Majority Leader Bill Frist and found nothing that immediately suggests a link to ricin, law enforcement sources said.** Investigators looked at postmarks, return addresses, and the contents of the letters. A lab in Maryland will now look for any traces of the lethal poison ricin on the letters. Capitol Police Chief Terrance W. Gainer said Wednesday that "no direct link" has been established between the poison found Monday afternoon, February 2, in the Dirksen Senate Office Building and that found in an intercepted letter addressed to the White House in November. Capitol Police said they had received neither a ricin threat nor a claim of responsibility. "This did come through the mail," Frist said Wednesday, adding that the powder was discovered in the cutting tray of the letter−opening machine in his office mailroom. **The Washington, DC, postal facility that handles congressional mail closed late Monday in response to the scare and was scheduled to reopen last night, postal officials said. U.S. Postal Service spokesman Gerry McKiernan said that 128 samples taken at two postal buildings came back negative for ricin.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A15862−2004Feb 5.html

12. *February 05, Congress Daily* — **Panel weighs expanded collective bargaining at Postal Service.** A debate over collective bargaining was at the center Wednesday of a Senate Governmental Affairs hearing on workforce issues in the U.S. Postal Service. The hearing was the Senate committee's third since the President's Commission on the Postal Service released a report in August suggesting changes for the mail service. In its report, the commission recommended, among other changes, that postal workers' health and retirement benefits be subject to collective bargaining, as wages for most postal employees already are. **Other workforce issues discussed at Wednesday's hearing included the commission's recommendations that the collective bargaining process include a mandatory mediation process; that the postal service be given greater rate−setting flexibility; and that the service be given greater authority to close low−performing post offices.**
Source: http://www.govexec.com/dailyfed/0204/020504cdam3.htm

[Return to top]

Agriculture Sector

13. *February 05, USAgNet* — **Irish consider country of origin labeling for poultry.** New legislation has been introduced in Ireland to ensure more information is made available at the point of sale to consumers of poultry meat. **The Irish Agriculture Minister, Joe Walsh, said the new legislation will require unprocessed poultry meat that is sold loose and which has been imported from outside the European Union to bear an indication of its country of origin.** This is already a requirement for pre−packaged poultry.
Source: http://www.usagnet.com/story−national.cfm?Id=126&yr=2004

14. *February 05, Associated Press* — **UN agencies back poultry vaccination.** United Nations agencies backed targeted poultry vaccination Thursday as part of a broader strategy to combat the bird flu ravaging Asia's farms, saying it could avoid some of the economically devastating consequences of mass slaughter. **Experts ending a two−day conference on the bird flu crisis said the epidemic is so widespread that some governments cannot afford to compensate farmers, many of whom are resisting killing off healthy birds.** They maintained that when it comes to infected birds, slaughter is the solution, but that under some circumstances vaccination of healthy birds could help stop the spread of the disease. Bird flu is decimating the poultry industry and the livelihoods of millions of small farmers in Asia. **More than 50 million chickens have been killed in an effort to stop the virus.** Ten governments are battling the disease, mostly by mass slaughter. Targeted vaccination can mean several things. "We can use targeted vaccinations, for example, to create a buffer zone around an infected province, or between two countries where one is infected and one is not," said Louise Fresco, assistant director general of the UN Food and Agriculture Organization. "Or even on large−scale farms, we could vaccinate in certain parts which have not yet been affected." It could also be an option for protecting breeding stocks, she added.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=541&ncid=751 &e=1&u=/ap/20040205/ap_on_he_me/bird_flu

15. *February 04, Reuters* — **Expert panel sees more U.S. cases of BSE. A panel of international experts said on Wednesday there was a "high probability" of more cases of bovine spongiform encephaopathy (BSE) in U.S. cattle.** The panel was appointed by Agriculture Secretary Ann Veneman after the United States' first case of the disease was reported in a cow in Washington state on December 23. **The experts noted there was a "high probability" that other infected cattle have been imported from Canada, and possibly Europe. Their report gave no details.** The infected U.S. cow was imported from Alberta, Canada in 2001. Panel chairman Urlich Kihm, who addressed a special meeting of U.S. Department of Agriculture officials, said the U.S. "could have a case a month" of mad cow disease. Kihm said he based that estimate on his own "logical thinking" and the experience of nations such as Denmark and Italy.
Source: http://www.washingtonpost.com/wp−dyn/articles/A12939−2004Feb 4.html

[Return to top]

Food Sector

16. *February 05, Stanford University Medical Center* — **Lingering bacteria may pose future food poisoning risks. Listeria bacteria, responsible for a lethal form of food poisoning, may escape the immune system by hiding out in the gall bladder of seemingly healthy**

people. The finding by researchers at Stanford University School of Medicine suggests that an unwitting food worker could transmit the bacteria to others by contaminating food products. "To have discovered a chronic carrier state in the gall bladder of an animal model, suggesting a potential source of food contamination, is important," said senior author Christopher Contag. **Until now, it had been thought that tainted food came primarily from infected animals or from soil or water harboring the hardy bacteria.** The researchers used a unique imaging technique to track the ebb and flow of Listeria infection in live mice. They tagged the bacteria with a luminescent molecule that can be non−invasively detected in living tissue, and then analyzed when and where Listeria showed up. The ability to visualize the whole animal enabled them to identify the gall bladder as an important bacterial resevoir, something they hadn't expected.
Source: http://www.alertnet.org/thenews/newsdesk/N05282883.htm

[Return to top]

Water Sector

Nothing to report.

[Return to top]

Public Health Sector

17. *February 05, New York Times* — **Human bird flu vaccine. Scientists have passed the first major hurdle in the complex process of developing an experimental bird flu vaccine for humans in case it is needed, an official of the World Health Organization (WHO) said.** The scientists are also working to develop a safer and easier test to detect the A(H5N1) strain of avian influenza now spreading across Asia. The steps are being taken as a precautionary measure because of fears that A(H5N1) might swap genes with a human strain to create a new one that could cause a worldwide epidemic, the WHO said. The chance of that occurring is considered low. To develop the vaccine and diagnostic test, three laboratories that are part of the WHO's influenza network are using a new method known as reverse genetics. **The aim is to develop a seed virus that the WHO could deliver within two months to drug companies that would make the human vaccine.** The technique involves substituting harmless influenza genes for the ones that make the strain lethal to birds. **Tuesday, two of the laboratories said that they had completed the first step in the reverse genetics technique and expected to begin testing the resulting virus in chickens and ferrets by next week.**
Source: http://www.nytimes.com/2004/02/05/health/05FLU.html

18. *February 05, Howard Hughes Medical Institute* — **Researchers determine reason for spread of 1918 influenza.** The explosive spread of the influenza virus during the 1918 pandemic that killed some 20 million people worldwide was likely enabled by the unique structure of a protein on the virus's surface, researchers are reporting. **The newly determined structure of the viral protein reveals that the 1918 strain of influenza underwent subtle alterations that enabled it to bind with efficiency to human cells, while retaining the basic properties of the avian virus from which it evolved.** According to the researchers, although their findings do not apply to the new strain of avian flu that is threatening to spread, they do emphasize how subtle

alterations in the influenza virus's infectivity could spawn a major epidemic.
Source: http://www.eurekalert.org/pub_releases/2004−02/hhmi−rdr02050 4.php

19. *February 04, Johns Hopkins University Bloomberg School of Public Health* — **Study questions premise of impending U.S. physician shortage. Physician groups, government agencies, and U.S. medical schools are concerned with a potential physician shortage and are calling for an increase in the number of physicians trained each year. However, new research from the Johns Hopkins Bloomberg School of Public Health found that the current U.S. physician supply is large enough to meet the needs of patients.** Jonathan Weiner, the study's author, compared the current supply of U.S. physicians with the staffing at several large medical group practices that treat health maintenance organizations (HMO) patients. He found that an increase in the number of physicians might not be necessary. The study found that the HMOs had about one physician for every 650 patients, compared with the current U.S. practicing physician supply of one per 400. Also, the HMOs tend to make greater use of primary care physicians rather than specialists. However, the study did identify a trend at the HMOs suggesting that specialist services increased at a faster rate than generalist care over the last two decades.
Source: http://www.eurekalert.org/pub_releases/2004−02/jhub−sqp02030 4.php

[Return to top]

Government Sector

20. *February 05, NBC30.com (Hartford, CT)* — **Governor pitches homeland security plan. Gov. John Rowland urged the Legislature Thursday, February 5, to fully fund his $70 million homeland security budget plan.** A 136−person team of volunteers is trained to respond to building collapses and other disasters. **Rowland's homeland security budget includes nearly $2.5 million for the team, which is comprised of police, fire and rescue personnel. It also includes environmental and hazardous material experts and civilians.** Rowland delivered his budget address Wednesday at the start of the legislative session. The three−term Republican presented a $14.2 billion plan that will need to cover the current fiscal year deficit, estimated between $40 million and $80 million. It also must account for a shortfall in the next fiscal year that could be as large as $200 million.
Source: http://www.nbc30.com/politics/2825333/detail.html

[Return to top]

Emergency Services Sector

21. *February 05, Firehouse.com* — **USFA Critical Infrastructure Protection Guide now available.** A new document that provides a comprehensive guide for all fire and emergency services is now available. **Prepared by the Emergency Management and Response−Information Sharing and Analysis Center (EMR−ISAC) to promote critical infrastructure protection, the Fire and Emergency Services Preparedness Guide for the Homeland Security Advisory System offers suggestions for activities that may be appropriate for the five Homeland Security Advisory System (HSAS) Levels.** Within this

guide, the emergency response leadership will find recommended preparedness measures for each HSAS Threat Condition. Therefore, the contents of the document should assist the heads of the fire and emergency medical services with the development and implementation of appropriate department or agency−specific preparedness measures. A complete copy of the guide can be seen and downloaded from the following link:
http://www.usfa.fema.gov/fire−service/cipc/cipc−jobaid.shtm
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=25691

[Return to top]

Information and Telecommunications Sector

22. *February 05, TechWeb* — **Security flaws found in popular firewall software. Flaws found late Wednesday in Check Point Software's popular firewall and VPN software could allow an attacker to gain entrance to enterprise networks, Internet Security Systems (ISS) said in a critical alert.** The disclosure of the vulnerabilities is yet another sign of a move by hackers to hammer at security software, firewalls, and intrusion detection systems, the very devices and applications enterprises rely on to defend themselves against intruders, said Dan Ingevaldson, the director of ISS's X−Force research team. The first vulnerability is within Check Point Firewall−1, and stems from the HTTP Application Intelligence that's designed to prevent potential attacks or detect protocol anomalies aimed at servers behind the firewall. The flaw also exists in the HTTP Security Server applications proxy that ships with all versions of Firewall−1, including the most recent. **On Wednesday, Check Point posted a patch for this vulnerability that it recommended be installed immediately.** The second vulnerability lies within Check Point VPN−1 Server and its virtual private networking (VPN) clients, Securemote and SecureClient. The vulnerability exists in the ISAKMP processing in both the server and clients, and if exploited, could result in an attacker gaining access to any client−enabled remote computer, including those in employees' homes.
Source: http://www.crn.com/sections/BreakingNews/dailyarchives.asp?A rticleID=47735

23. *February 05, US−CERT* — **Technical Cyber Security Alert TA04−036A: HTTP Parsing Vulnerabilities in Check Point Firewall−1.** The Application Intelligence (AI) component of Check Point Firewall−1 is an application proxy that scans traffic for application layer attacks once it has passed through the firewall at the network level. **Both the AI and HTTP Security Server features contain an HTTP parsing vulnerability that is triggered by sending an invalid HTTP request through the firewall**. When Firewall−1 generates an error message in response to the invalid request, a portion of the input supplied by the attacker is included in the format string for a call to sprintf(). **It is possible to exploit this format string vulnerability to execute commands on the firewall**. This vulnerability can be exploited as a heap overflow, which would allow an attacker to execute arbitrary code. In either case, the commands or code executed by the attacker would run with administrative privileges, typically "SYSTEM" or "root". Additional information and a patch are available on the Check Point Website:
http://www.checkpoint.com/techsupport/alerts/security_server .html
Source: http://www.us−cert.gov/cas/techalerts/TA04−036A.html

Internet Alert Dashboard

Current Alert Levels

AlertCon: 2 out of 4 https://gtoc.iss.net	Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_MYDOOM.A** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 1434 (ms−sql−m), 137 (netbios−ns), 6129 (dameware), 445 (microsoft−ds), 1080 (socks), 3128 (squid−http), 3127 (mydoom), 80 (www), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

24. *February 05, The Business Times: Shipping Times* — **Armed pirates attack cargo ship at Yemen.** Pirates armed with shotguns tried to board a general cargo ship at a Yemeni oil terminal in the Gulf of Aden, on Sunday, February 1, where terrorists attacked the tanker Limburg in 2002, the International Maritime Bureau's Piracy Reporting Center said. The four robbers fled in speedboats after making several attempts to board the vessel at the Ash Shihr oil terminal on January 29, the IMB said. The incident was one of eight during the week ended February 4. **Piracy attacks on ships worldwide rose 20 per cent last year to 445, the second−highest number of incidents reported in more than a decade, according to the center, which is part of the International Chamber of Commerce's Commercial Crime Services unit.** Two days earlier, four speedboats carrying masked pirates approached a chemical tanker off Indonesia. The attackers fled after the vessel's crew shone searchlights on them. On the same day, an oil tanker came under attack from robbers with knives at the Indonesian oil port of Balikpapan. The pirates fled with two life craft, the IMB said. A container ship and a bulk carrier, a ship used to haul grain and iron−ore, were attacked in the Singapore Strait on January 29. Two other vessels off Nigeria and Haiti were also involved in last week's attacks.
Source: http://business−times.asia1.com.sg/story/0,4567,107214,00.ht ml

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.